An A_5 Galois action on a class
of elliptic dessins d'enfants

David S. Burggraf

Department of Mathematics, University of British Columbia
Vancouver, B.C. V6T 1Z2, Canada

Abstract

As noted in [Jon97], only examples of solvable Galois actions on classes of dessins d'enfants have been explicitly constructed. In this paper an action of the nonsolvable alternating group A_5, represented as a Galois group, on a class of elliptic dessins is presented.

1 Introduction

A Belyĭ function β defined on a compact Riemann surface X is a meromorphic covering of the Riemann sphere $\Sigma = \mathbb{C} \cup \{\infty\}$ with all branch points contained in $\{0, 1, \infty\}$. Belyĭ functions β that satisfy the additional condition that all points in the pre-image of 1 are ramified with ramification order equal to 2, are called *clean* Belyĭ functions. It is common practice to extend the definition of a Belyĭ function to a projective algebraic curve $\mathcal{C}$ by identifying $\mathcal{C}$ with its underlying compact Riemann surface. One can associate a bipartite graph $\mathcal{G}(\beta)$ to the Belyĭ pair $(\mathcal{C}, \beta)$ by using β to lift the closed unit interval $I = [0, 1] \subset \mathbb{C} \cup \{\infty\}$; label the points in $\beta^{-1}(I)$ lying above 0 and 1, respectively, by black and white vertices, respectively. Each connected component in the inverse image $\beta^{-1}(0, 1)$ is an *edge segment* joining two vertices of opposite type and each connected component of $\mathcal{C} \backslash \beta^{-1}(I)$ is a simply connected region, which will be referred to as a face. A bipartite map $\mathcal{M}$ on $\mathcal{C}$ consists of a bipartite graph $\mathcal{G}$ lying on $\mathcal{C}$ together with the faces of $\mathcal{C} \backslash \mathcal{G}$. A bipartite map on a compact Riemann surface obtained by lifting I by a clean Belyĭ funtion is denoted by $\mathcal{D}(\beta)$, and belongs to an important class of combinatorial objects known as dessins d'enfants.

Belyĭ's theorem [Bel79] states that a projective algebraic curve $\mathcal{C}$ is defined over the algebraic numbers $\overline{\mathbb{Q}}$ if and only if there exists a Belyĭ function $\beta : \mathcal{C} \to \mathbb{P}^1(\mathbb{C}) = \mathbb{C} \cup \{\infty\}$. Inspired by Belyĭ's theorem, Alexander Grothendieck [Gro97] observed that the absolute Galois group $\Gamma = \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ acts naturally on Belyĭ pairs $(\mathcal{C}, \beta)$ and induces a faithful action on the corresponding dessins. This action of Γ on dessins lends direct geometrical insight into the intractible group Γ and is the basis of an ambitious program started by Grothendieck aiming at a complete description of the absolute Galois group.

In the survey paper [Jon97] some explicit examples of nontrivial Galois actions on dessins lying on: the Riemann sphere, elliptic curves, and hyperelliptic curves are given. In these examples, the Galois groups acting were solvable,

namely: cyclic groups and the metabelian affine group $AGL_1(p)$. This leads to the natural generalization suggested by the author in the last sentence of the paper: to produce explicit examples of nontrivial Galois actions on classes of dessins where more complicated Galois groups are acting such as nonsolvable groups or solvable groups with unbounded derived length. In this paper, the simplest nonsolvable group A_5 is explicitly shown to have a nontrivial Galois action on a class of elliptic dessins.

2   Elliptic Dessins

It can be verified using a computer algebra program such as [GAP] that the separable polynomial $f(x) = x^{12} - \frac{12}{11}x^{11} + 1$ is irreducible over $\mathbb{Q}$, and the Galois group $G = \text{Gal}(\mathbb{Q}, f)$ of its splitting field over $\mathbb{Q}$ is S_{12}. The zeros of $f(x)$ are displayed in Figure 1 and labelled for later reference.
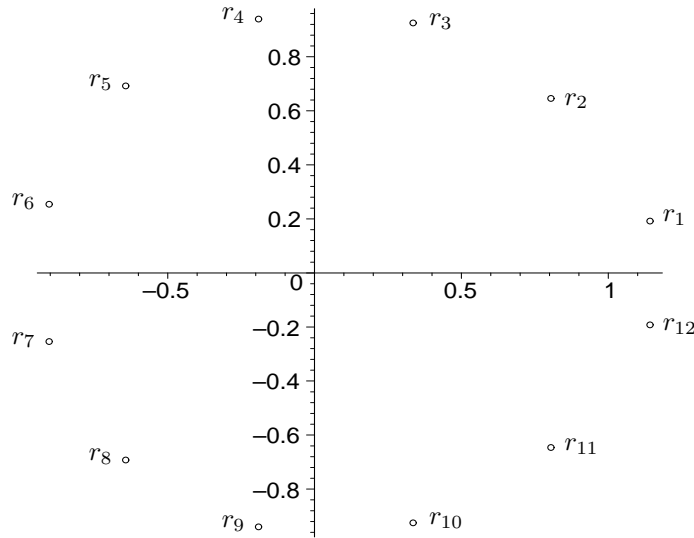

Figure 1:   The labelling of the zeros of the polynomial $f(x)$

Consider the elliptic curve

$$E_{i,j,k} = \left\{ [x, y, z] \in \mathbb{P}^2(\mathbb{C}) \,|\, y^2 z - (x - r_i z)(x - r_j z)(x - r_k z) = 0 \right\}, \quad (1)$$

where r_i, r_j, and r_k are distinct zeros of the polynomial $f(x)$. It is customary, when defining a Belyǐ function on a projective algebraic curve $\mathcal{C}$, to "affinize" the curve $\mathcal{C}$ by considering only the the part of $\mathcal{C}$ contained in the open neighbourhood of $\mathbb{P}^2(\mathbb{C})$ where $z \neq 0$. Thus, only the homogeneous coordinates of the form $[x, y, 1]$ in $\mathcal{C}$ are considered, and identifying these with the affine coordinates (x, y), yields the associated affine curve $\mathcal{C}^{aff}$. The projective curve is then

easily recovered from the affine one by "homogenizing" it's defining polynomial. Therefore, we will restrict our attention to the affine elliptic curve

$$E_{i,j,k}^{aff} = \left\{ (x,y) \in \mathbb{C}^2 \,|\, y^2 = (x - r_i)(x - r_j)(x - r_k) \right\}$$

and make the identification $E_{i,j,k} = E_{i,j,k}^{aff} \cup \infty$, where ∞ corresponds to the point $[0,1,0] \in \mathbb{P}^2(\mathbb{C})$. The mapping $\pi^{i,j,k} : E_{i,j,k} \to \Sigma$ defined by $\pi^{i,j,k}(x,y) = x$ is a degree 2 covering of Σ with branch points r_i, r_j, r_k, and ∞, bearing in mind that $(\pi^{i,j,k})^{-1}(\infty) = [0,1,0] = \infty$. These branch points are in turn sent to $0, 0, 0$, and ∞, respectively, by the polynomial $f(x)$. In addition, $f(x)$ has two ramification points 0 and 1 lying above the branch points 1 and $\frac{10}{11}$, hence $f \circ \pi^{i,j,k}$ has a total of four branch points $\{0, \frac{10}{11}, 1, \infty\}$. We will now make use of the well known Belyĭ function $\beta_{m,n}$ (see [JS96]), where $m = 10, n = 1$, as it is ideally suited to handle the present situation. The function $\beta_{m,n} : \Sigma \to \Sigma$ is defined by

$$\beta_{m,n}(x) = \frac{(m+n)^{m+n}}{m^m n^n} x^m (1-x)^n.$$

It can be easily verified that $\beta_{m,n}$ is unramified outside $\{0, \frac{m}{m+n}, 1, \infty\}$ and sends this set into $\{0, 1, \infty\}$. Therefore, the composition $\phi = \beta_{10,1} \circ f \circ \pi^{i,j,k}$ is a Belyĭ function, and furthermore, $\beta^{i,j,k} = \beta_{1,1} \circ \phi$ is a clean Belyĭ function, i.e., has ramification order equal to 2 at each point in the pre-image of 1. The lift of the unit interval $I = [0,1] \subset \Sigma$ by $\beta^{i,j,k}$ gives rise to an elliptic dessin $\mathcal{D}(\beta^{i,j,k})$ (see Figure 3).

3   Monodromy Groups

Let $\beta : \mathcal{C} \to \Sigma$ be a branched covering of the Riemann sphere, and suppose $B = \{b_0, \ldots, b_k\} \subset \Sigma$ is the set of branch points. Fix a base point $p \in \Sigma - B$, and let $\Omega = \beta^{-1}(p)$ denote the fiber above p in $\mathcal{C}$. The fundamental group $\Pi = \pi_1(\Sigma - B, p)$ acts naturally on Ω and has a presentation given by

$$\Pi = \langle \alpha_0, \ldots, \alpha_k \,|\, \prod_{i=0}^{k} \alpha_i = 1 \rangle,$$

where each generator α_i is the homotopy class of a suitably chosen loop based at p, that winds once around b_i. For any element $p_r \in \Omega$, each element $\alpha_i \in \Pi$ lifts to a unique homotopy class of paths in $\mathcal{C}$, such that any representative path in the homotopy class starts at p_r and ends at some common point $p_s \in \Omega$. This defines a bijective mapping $g_i : \Omega \to \Omega$, which gives a permutation representation $\rho : \Pi \to S_\Omega$, defined by $\rho(\alpha_i) = g_i$, where S_Ω is the symmetric group on the set Ω. The permutation g_i $(0 \leq i \leq k)$ has $n_i = |\beta^{-1}(b_i)|$ disjoint cycles, each having cycle length l_{ir} $(1 \leq r \leq n_i)$. Each disjoint cycle of g_i corresponds to a ramification point of order l_{ir} on $\mathcal{C}$ lying above b_i, where l_{ir} sheets of $\mathcal{C}$ come together. The resulting permutation group $G(\beta) = \rho(\Pi)$

is called the monodromy group of the branched covering β. In the case that β is a Belyĭ function, we have $B \subset \{0, 1, \infty\}$, and $G(\beta)$ generated by the two permutations g_0 and g_1. Moreover, if β is a clean Belyĭ function, all ramification points above 1 have ramification order equal to 2, hence all disjoint cycles of g_1 have length $l_{1r} = 2$ $(1 \le r \le n_1)$, and the monodromy group $G(\beta)$ has the following partial presentation

$$G(\beta) = \langle g_0, g_1 \,|\, g_0^l = g_1^2 = 1, \mathrm{ETC} \rangle,$$

where l is the least common multiple of $\{l_{0r}\}_{r=1}^{n_0}$.

The monodromy group $G(\beta)$ has an important connection to the graph $\mathcal{G}(\beta)$ associated to β; in fact, when β is a clean Belyĭ function, the conjugacy class of the monodromy group $G(\beta)$ in S_Ω completely determines the graph-isomorphism class of $\mathcal{G}(\beta)$ and vice versa. Suppose the base point $p \in \Sigma - B$ is chosen to lie in the open interval $(0, 1)$, then each edge segment e_r of $\mathcal{G}(\beta)$ contains exactly one point $p_r \in \Omega$ and is incident to a unique black vertex at one end and a white vertex at the other. Each disjoint cycle of the monodromy generator g_0 describes how the point p_r is cyclically permuted in Ω around a ramification point v lying above 0, and thus describes how the edge segment e_r is cycled (according to the orientation of $\mathcal{C}$) around its incident black vertex v. The valency of v is then given by the length l_{0r} of the disjoint cycle. This describes the connection between the black vertices of $\mathcal{G}(\beta)$ and the disjoint cycles of g_0, and a similar connection exists between the disjoint cycles of g_1 and the white vertices. In the case that β is a clean Belyĭ function, the edge segments come in pairs with a white vertex of valency equal to 2 between them. The union of a white vertex together with its pair of incident edge segments is called an *edge* and each edge corresponds to a unique disjoint 2-cycle of g_1. Thus, the black vertices and edges of $\mathcal{G}(\beta)$ are determined by the disjoint cycles of g_0 and g_1, respectively, and vice versa.

Figure 2 displays the graphs $\mathcal{G}(\beta_{1,1})$ and $\mathcal{G}(\psi)$, where $\psi = \beta_{1,1} \circ \beta_{10,1}$, obtained by lifting the graph $\mathcal{G}_1$, which consists of a single edge $(0, 1)$, a black vertex located at 0, and a white vertex located at 1. The graphs $\mathcal{G}(\beta_{1,1})$ and $\mathcal{G}(\psi)$ are shown in relation to the lifts of rotations about 0 and 1 based at $p = \frac{1}{2}$, represented by the dashed and dotted loops, respectively. With the labelling of the points in $\Omega = \beta_{1,1}^{-1}(p)$ and $\tilde{\Omega} = \psi^{-1}(p)$ as in the figure, we have the following monodromy generators:

$$\begin{aligned} G(\beta_{1,1}) : g_0 &= (1)(2), \\ g_1 &= (1, 2). \end{aligned}$$

$$\begin{aligned} G(\beta_{1,1} \circ \beta_{10,1}) : \tilde{g}_0 &= (1, 2, 3, 4, 5, 6, 7, 8, 9, 10)(11, 21), \\ \tilde{g}_1 &= (1, 11)(2, 12)(3, 13)(4, 14)(5, 15)(6, 16) \\ &\quad (7, 17)(8, 18)(9, 19)(10, 20)(21, 22). \end{aligned}$$
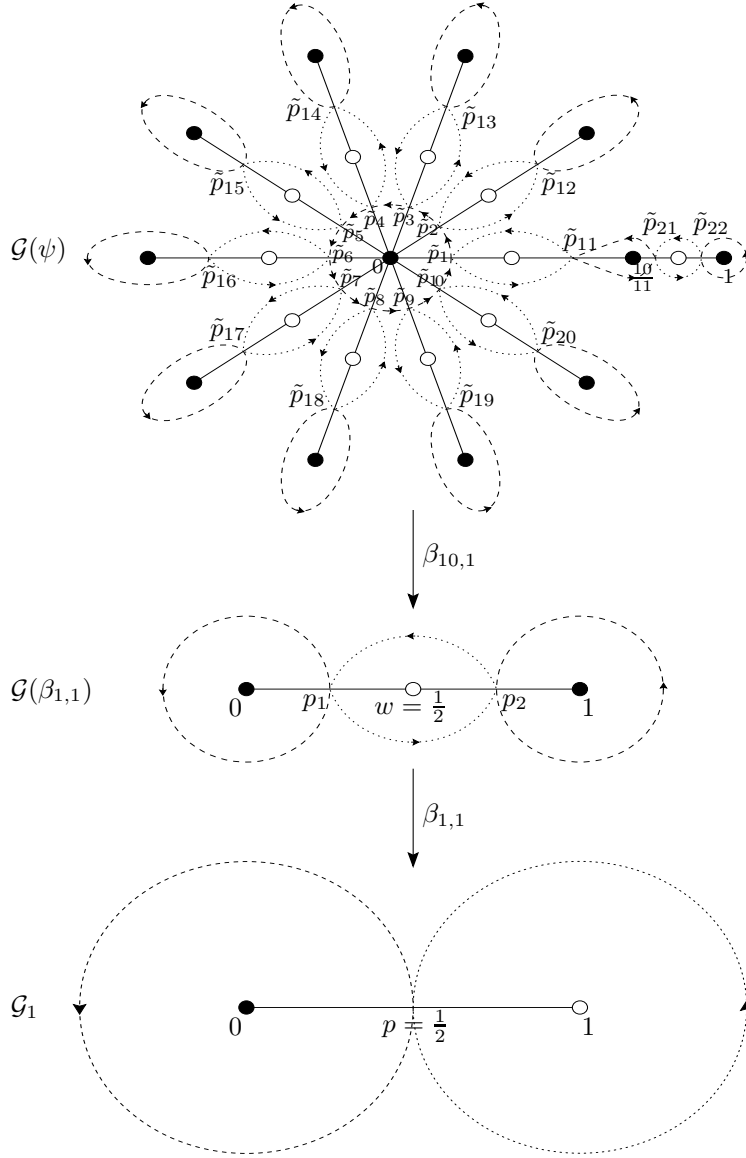
Figure 2: The graphs $\mathcal{G}(\beta_{1,1})$ and $\mathcal{G}(\psi)$ obtained by lifting the graph $\mathcal{G}_1$.

The Belyĭ function $\beta_{1,1}$ is clean and has only one ramification point located at the white vertex $w = \frac{1}{2} \in \mathcal{G}(\beta_{1,1})$, corresponding to the only disjoint 2-cycle of g_1. The ramification order at w is the cycle length $l_{1,1} = 2$, which accounts for the two copies of $\mathcal{G}_1$ emanating from w. The Belyĭ function ψ is also clean and $\mathcal{G}(\psi)$ has two copies of $\mathcal{G}_1$ emerging from every white vertex. In addition, ψ has two ramification points at the black vertices located at 0 and $\frac{10}{11}$ in $\mathcal{G}(\psi)$, corresponding to the two non-trivial cycles of $\tilde{g}_0$. The black vertex located at 0 in $\mathcal{G}(\psi)$ corresponds to the 10-cycle in $\tilde{g}_0$ and has valency $\tilde{l}_{01} = 10$. This accounts for the 10 copies of $\mathcal{G}(\beta_{1,1})$ emanating from 0, forming a floral pattern in $\mathcal{G}(\psi)$ centered at 0, which will be referred to as a 10-fold $\mathcal{G}(\beta_{1,1})$-bouquet. The black vertex at $\frac{10}{11} \in \mathcal{G}(\psi)$ corresponding to the 2-cycle of $\tilde{g}_0$, has valency $\tilde{l}_{02} = 2$ and is the center of a 2-fold $\mathcal{G}(\beta_{1,1})$-bouquet.

Figure 3 shows the graphs $\mathcal{G}(\psi \circ f)$ and $\mathcal{G}(\beta^{2,7,11})$ obtained by lifting $\mathcal{G}(\psi)$ by f and $f \circ \pi^{2,7,11}$, respectively. Unlike the previous figure, the dashed and dotted lines representing the lifts of rotations about 0 and 1 have been omitted, in order to emphasize the graphs; however, no monodromy information is lost by doing so, because $G(\beta^{2,7,11})$ is determined up to conjugacy by $\mathcal{G}(\beta^{2,7,11})$. The ramification point of f at $v = 1$ lies above the black vertex $f(1) = \frac{10}{11} \in \mathcal{G}(\psi)$, which joins a 10-fold $\mathcal{G}(\beta_{1,1})$-bouquet to the left and a 1-fold $\mathcal{G}(\beta_{1,1})$-bouquet to the right. Since v has ramification order equal to 2, a lift of a neighbourhood of $\frac{10}{11} \in \mathcal{G}(\psi)$ by f to a neighborhood of v yields two 10-fold $\mathcal{G}(\beta_{1,1})$-bouquets and two 1-fold $\mathcal{G}(\beta_{1,1})$-bouquets emanating from v. This accounts for two copies of $\mathcal{G}(\psi)$ in $\mathcal{G}(\psi \circ f)$, which intersect at v; one starting at 0, which passes through v and proceeds downward, and the other starting at $\frac{12}{11}$, which passes through v and proceeds upward. The ramification point of f at $0 \in \mathcal{G}(\psi \circ f)$ has ramification order equal to 11 and lies above $f(0) = 1$, giving rise to the 11-fold $\mathcal{G}(\psi)$-bouquet centered at 0. The central black vertices of the twelve 10-fold $\mathcal{G}(\beta_{1,1})$-bouquets in $\mathcal{G}(\psi \circ f)$ are the zeros $\{r_1, \ldots, r_{12}\}$ of f and are ordered according to Figure 1. The projection $\pi^{2,7,11}$ is ramified over only three points of $\mathcal{G}(\psi \circ f)$: r_2, r_7, and r_{11}, each having ramification order equal to 2. Hence, $\pi^{2,7,11}$ lifts each of the three 10-fold $\mathcal{G}(\beta_{1,1})$-bouquets centered at r_2, r_7, and r_{11}, to 20-fold $\mathcal{G}(\beta_{1,1})$-bouquets in $\mathcal{G}(\beta^{2,7,11})$. Since $\pi^{2,7,11}$ is a degree 2 covering and is unbranched away from $\{r_2, r_7, r_{11}\}$, the remaining nine 10-fold $\mathcal{G}(\beta_{1,1})$-bouquets in $\mathcal{G}(\psi \circ f)$ are each lifted to two distinct 10-fold $\mathcal{G}(\beta_{1,1})$-bouquets giving a total of eighteen 10-fold $\mathcal{G}(\beta_{1,1})$-bouquets in $\mathcal{G}(\beta^{2,7,11})$. The dessin $\mathcal{D}(\beta^{2,7,11})$ consists of the graph $\mathcal{G}(\beta^{2,7,11})$ and a single face lying on the torus obtained by identifying the opposite sides of a square, as shown at the top of Figure 3.

4 Galois Actions on Dessins

A_5 is the orientation preserving symmetry group of the regular dodecahedron and its action on the faces yields a permutation representation $A_5 \rightarrow S_{12}$. With the faces labelled as in Figure 4, A_5 is given the following presentation:

$$A_5 = \langle a, b \,|\, a^5 = b^3 = (ab)^2 = 1 \rangle,$$

$\mathcal{D}(\beta^{2,7,11})$

$\pi^{2,7,11}$

$\mathcal{G}(\psi \circ f)$

0 1 $\frac{12}{11}$
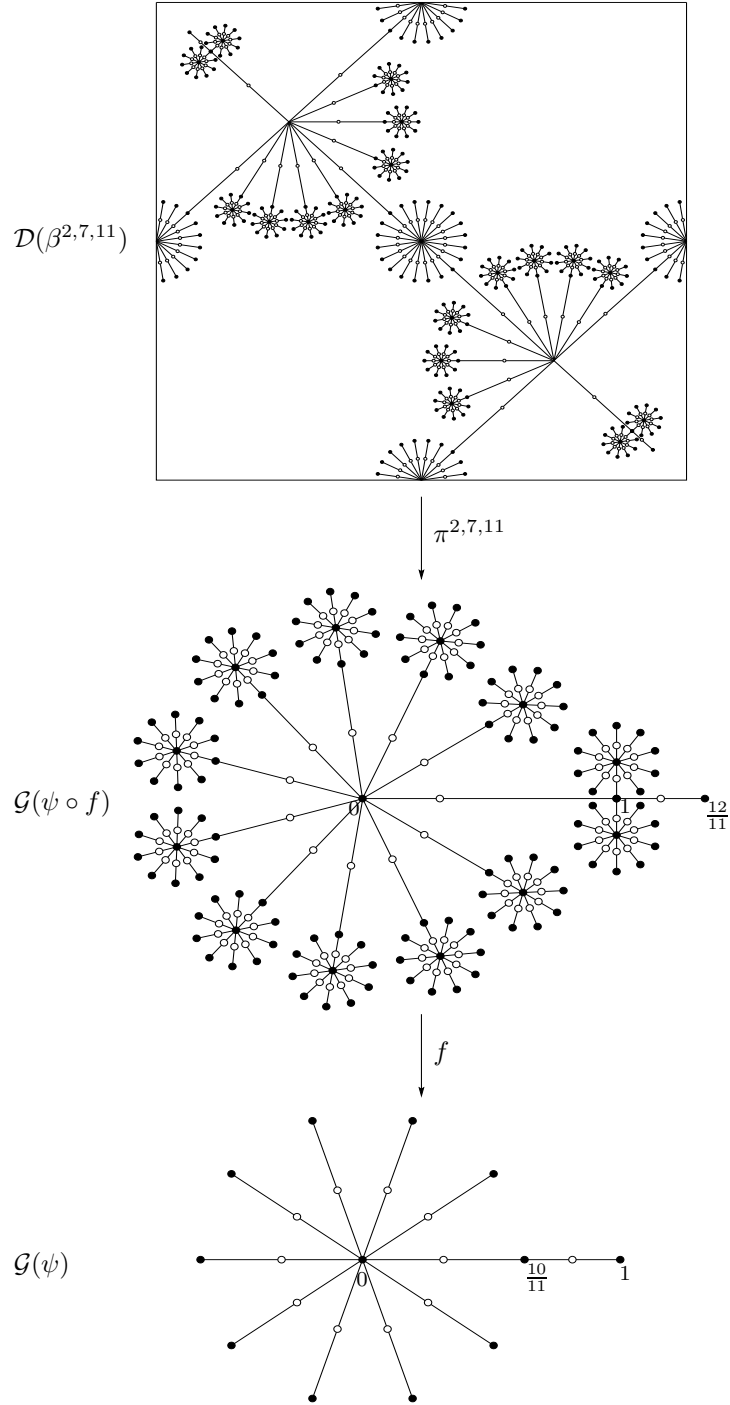
f

$\mathcal{G}(\psi)$

0 $\frac{10}{11}$ 1

Figure 3: The elliptic dessin $\mathcal{D}(\beta^{2,7,11})$ obtained by lifting the graph $\mathcal{G}(\psi \circ f)$ by $\pi^{2,7,11}$.

where

$$a = (2,3,4,5,6)(7,8,9,10,11),$$
$$b = (1,2,3)(4,6,7)(5,11,8)(9,10,12),$$
$$ab = (1,2)(3,6)(4,11)(5,7)(8,10)(9,12).$$

Figure 4: Two views of the dodecahedron are shown; the view on the right is a rotation of the view on the left by π radians about the vertical axis. In both views, 12 is assigned to the hidden face at the bottom.

By taking the ordering of the roots $\{r_i\}_{i=1}^{12}$ of $f(x)$ in Figure 1, and identifying the ith root with the ith face of the dodecahedron, we get a Galois representation $A_5 \to G$.

Let $\mathcal{E}$ be the family of all elliptic curves $E_{i,j,k}$ as in (1), then $G = \mathrm{Gal}(\mathbb{Q}, f)$ acts on $\mathcal{E}$ as follows: an automorphism $\sigma \in G$ takes $E_{i,j,k}$ to a conjugate curve $E_{i,j,k}^{\sigma}$ defined by

$$E_{i,j,k}^{\sigma} = \left\{ [x,y,z] \in \mathbb{P}^2(\mathbb{C}) \,|\, y^2 = (x - \sigma(r_i)z)(x - \sigma(r_j)z)(x - \sigma(r_k)z) \right\}.$$

By identifying the ith root r_i with its index i, we have and induced action of σ on the triple (i,j,k), allowing us to rewrite $E_{i,j,k}^{\sigma}$ in the form

$$E_{i,j,k}^{\sigma} = \left\{ [x,y,z] \in \mathbb{P}^2(\mathbb{C}) \,|\, y^2 = (x - r_{\sigma(i)}z)(x - r_{\sigma(j)}z)(x - r_{\sigma(k)}z) \right\}.$$

So the action of σ on the triple (i,j,k) induces an action on the elliptic curve $E_{i,j,k}$, and further, induces an action on the dessin $\mathcal{D}(\beta^{i,j,k})$ associated to the Belyĭ pair $(E_{i,j,k}, \beta^{i,j,k})$. For example, $a : E_{2,7,11} \mapsto E_{3,8,7} = E_{3,7,8}$, which induces the action $a : D(\beta^{2,7,11}) \mapsto D(\beta^{3,7,8})$. Moreover, the orbits containing the triple $(2,7,11)$ under the action of the subgroups $<a>$, $<b>$, and $<ab> \subset A_5$ are as follows:

$$<a> : \ \{(2,7,11),(3,7,8),(4,8,9),(5,9,10),(6,10,11)\},$$
$$<b> : \ \{(2,7,11),(3,4,8),(1,5,6)\},$$
$$<ab> : \ \{(2,7,11),(1,4,5)\}.$$

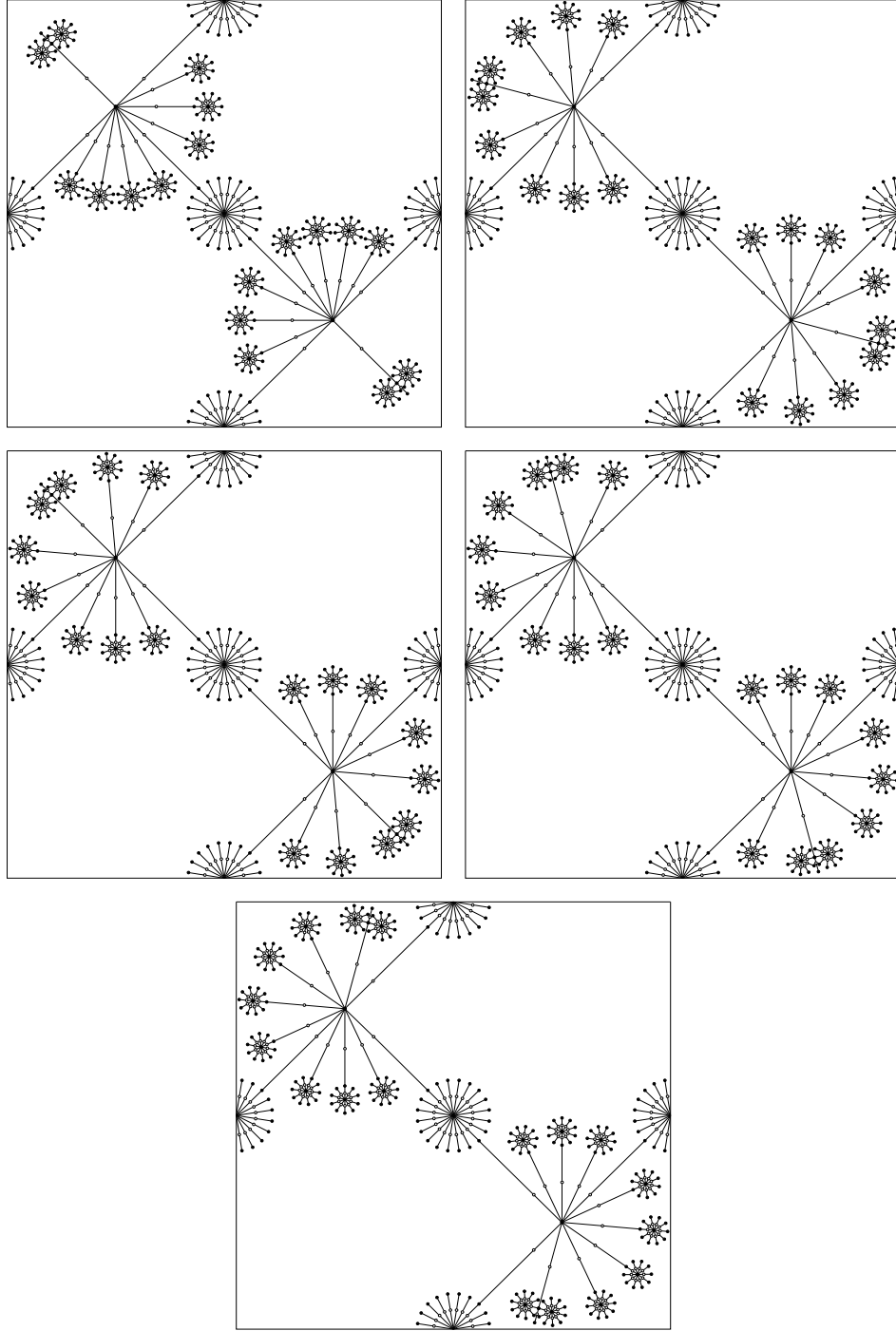The orbits of the corresponding dessins are illustrated in Figures 5, 6, and 7.

Figure 5: The orbit of the dessin $\mathcal{D}(\beta^{2,7,11})$ under the action of $<a>\subset G$, shown from left to right as successive powers of a act on $\mathcal{D}(\beta^{2,7,11})$.
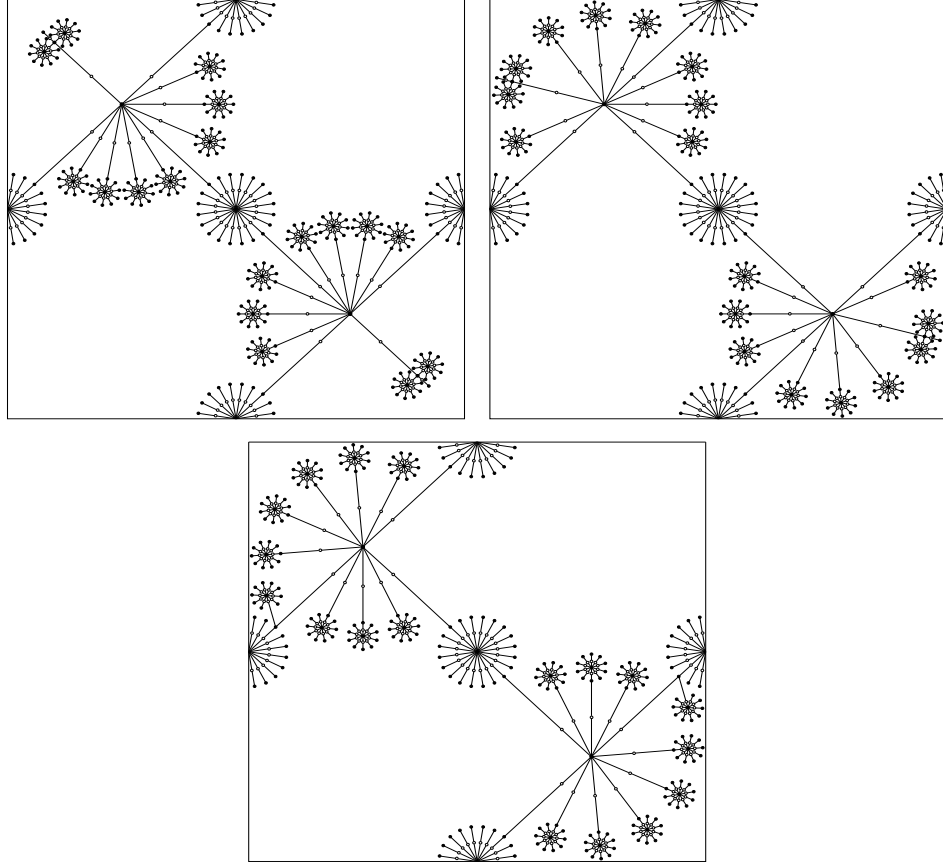
Figure 6: The orbit of the dessin $\mathcal{D}(\beta^{2,7,11})$ under the action of $<b>\subset G$, shown from left to right as successive powers of b act on $\mathcal{D}(\beta^{2,7,11})$.
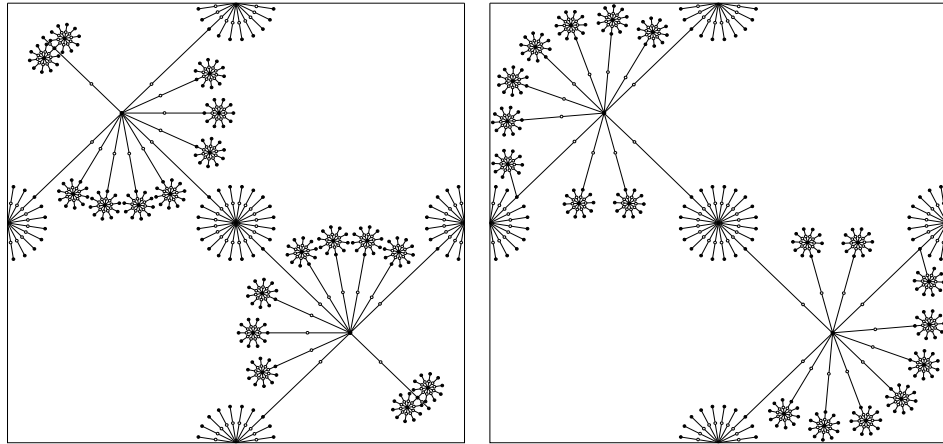

Figure 7: The action of ab on the dessin $\mathcal{D}(\beta^{2,7,11})$.

References

[Bel79] G. V. Belyĭ. On galois extensions of a maximal cyclotomic field. *Izv. Akad. Nauk SSSR*, 43:269–276 (Russian), 1979. [Math. USSR Izvestiya 14 (1980), 247-256 (English translation)].

[GAP]   The GAP Group, GAP — Groups, Algorithms, and Programming, Version 4b5, 1998. School of Mathematical and Computational Sciences, University of St Andrews, North Haugh, St Andrews, Fife KY16 9SS, Scotland and Lehrstuhl D für Mathematik, Rheinisch Westfälische Technische Hochschule, Aachen, Germany.

[Gro97] A. Grothendieck. Esquisse d'un programme, typescript (1984). In *Geometric Galois Actions*. London Math. Soc. Lecture Note series, Cambridge University Press, 1997.

[Jon97] Gareth A. Jones. Maps on surfaces and galois groups. *Mathematica Slovaca*, 47(1):1–33, 1997.

[JS96]   G. A. Jones and D. Singerman. Belyĭ functions, hypermaps and galois groups. *Bull. London Math. Soc.*, 28:561–590, 1996.